Requirements for Risk Assessment Tools for Aircraft Electrical Interconnection Subsystems

Dr. Christopher Smith
FAA William J. Hughes Technical Center
AAR-430
Atlantic City International Airport
NJ 08405, United States

and

Mr. Robert Pappas
FAA William J. Hughes Technical Center
AAR-433
Atlantic City International Airport
NJ 08405, United States

Background

The continued safe operation of aircraft well into their expected service life depends on the safe and effective transfer of electrical power and signals between aircraft electrical devices. This in turn requires the enduring physical integrity of the electrical interconnect subsystem (EIS), which is comprised predominately by wire, connectors, switching devices (including relays and solid state switches) and protective devices such as circuit breakers. Recently there has been speculation that, under some conditions, the EIS on older aircraft may degrade to the point that it is no longer capable of ensuring the safe transfer of electrical current.

Though an EIS may be optimal with respect to aircraft design requirements, operational assumptions and the data existing at the time of certification, unanticipated demands on the EIS and changes to aircraft configuration can degrade EIS performance below acceptable limits. In addition, performance characteristics of the EIS over service lives of more than twenty years are difficult to predict. Inevitably, unanticipated failure modes will emerge requiring remedial action.

The EIS in modern transport aircraft provides the means of communication and/or power for nearly every subsystem aboard the aircraft. Failures in the EIS could result in the loss of critical functions as well as the potential for fire or other physical damage to the aircraft. Hence, the FAA is conducting a number of research projects addressing aging EIS concerns. The particular focus of one project is the development of advanced EIS risk assessment tools for design optimization and life-cycle management.

EIS Design Requirements and Risk Assessment

Certification requires that systems on airplanes be able to perform their intended function under all foreseeable conditions. The probabilistic safety analysis required under Part 25 (Para. 25.1309(b)) is just one of the requirements that all the systems on the airplane must meet. These analyses define the safety criticality of individual systems based on the functions they perform and requires a numerical assessment (based on a typical flight) of those systems that can participate in safety critical functions. The safety analysis done for certification is not a risk assessment in the truest sense of the word. For example, it does not take into account such things as fleet size when considering total exposure to an event. Typically, the various systems safety analysis done to satisfy 25.1309(b) have addressed the individual wires as parts of the various systems they serve, not as an individual subsystem that supports all the systems on the airplane. The EIS, in general, is designed and certified based on the individual systems needs, the fire marshal's requirement for the compartment the wire goes through, and good wiring practice (as defined in documents such as AC 43-13B). The fact the EIS has meet all requirements is not documented in one place.

Modern transport aircraft, with their digital systems and increased use of electrical and electronic command and control systems, are designed and certified to bound the risk associated with critical failure of one or more aircraft systems. The ever increasing complexity of these systems and the availability of more precise risk assessment methodologies (and the computational resources to implement them) have lead to a more sophisticated certification analysis than that applied to older generation aircraft. Federal Aviation Regulation

Paper presented at the RTO AVT Specialists' Meeting on "Life Management Techniques for Ageing Air Vehicles", held in Manchester, United Kingdom, 8-11 October 2001, and published in RTO-MP-079(II).

(FAR) 25.1309[1] identifies risk requirements and its companion Advisory Circular (AC 25.1309) interprets those requirements as the familiar 10^{-9} probability of catastrophic failure. The regulation also lays out other specific risk requirements and means to verify adherence to those requirements. AC 25.1309 and SAE Aerospace Recommend Practice (ARP) 4761 further elaborate on acceptable means of demonstrating compliance with FAR 25.1309.

First and second generation jet aircraft subsystems, on the other hand, were typically evaluated to specific, independent design or performance requirements – to the single-fault criterion or to a basic fail-safe design concept. The certification basis for older aircraft may not necessarily provide for an adequate assessment of risk associated with EIS failure, particularly when these airplanes are operated beyond their original design life or if they are updated with modern electronic/electrical systems. Unfortunately, qualitative analyses, which work well for simple subsystems, can breakdown when thousands of potential failures modes interact to produce consequences with unknown probability of occurrence.

For aircraft in the design stage, the means for demonstrating compliance to FAR 25.1309 or earlier requirements range from rather simple (qualitative arguments proposing an analogy to similar, already-certified subsystems) to complex (use of formal quantitative fault tree analysis and failure modes and effects analysis). Many of the more sophisticated analysis methodologies rely on multiple-cause failure condition evaluations using sophisticated probability tools. In all cases, the availability of precise design information is assumed.

FAR 25.1309

AC 25.1309 identifies a process that begins with a Functional Hazard Assessment (FHA) and then concludes with a safety assessment whose initial objectives are defined by the FHA. A FHA is a highly methodical and structured analysis of the functions performed by the aircraft and the aircraft systems that identifies all single failure conditions and combinations of failures and failure conditions that could hazard the aircraft. The FHA does not attempt to determine the cause of the functional failure. Instead, the purpose of the analysis is to identify the effects of the loss of each particular function and also the effects of the improper operation of the function (malfunction) and to classify the severity of the effects. The loss or inability to properly perform a function is considered to be a failure condition. The classification of the severity of each failure condition is based on the effect on the airplane and it's occupants. Failure conditions are classified as minor, major, hazardous, or catastrophic.

The FHA is a qualitative analysis, usually conducted using service experience, engineering and operational judgment. In some cases, the effects of the loss or malfunction cannot be accurately estimated. The FHA will then describe the type of tests that will be used to evaluate the severity of the failure condition. The FHA should consider all phases of flight, environmental conditions and abnormal/emergency operating conditions.

For systems where there is a clear correlation between functions and the system that performs the function, and where the systems (and hence functional) interrelationships are relatively simple, it may be feasible to conduct a separate relatively unstructured FHA for each system. The EIS does not, however, fall into this category. The EIS, like electrical, hydraulic, and pneumatic power systems do not directly perform aircraft functions. These systems provide services necessary for the operation of other systems; their loss or malfunction usually have widespread effects on many other aircraft systems. For the EIS a structured, top-down approach from an airplane perspective should be used. The FHA must also consider all factors that might alleviate or intensify the direct effects of the initial failure condition.

Figure 1 is a graphical representation of the development and manifestation of failures and failure conditions. Any FHA which fails address all of these factors is incomplete.

The system safety assessment uses various tools to assess the probability of occurrence associated with the failure conditions derived from the FHA. This analysis may be either qualitative or quantitative. Because the

---

[1] FAR 25.1309 was originally issued in 1965 with no reference to probability of failure, severity of failure, or aircraft safety risk. In 1970, FAR 25.1309 was amended to incorporate the concept of risk. The risk basis was further clarified in a 1977 amendment. FAR 25.1309 is currently being revised as part of the FAA/JAA Harmonization activities.

failure of an EIS can affect multiple flight critical systems, designers of new or highly modified EISs are usually compelled to apply sophisticated analysis techniques including FMEA, Fault Tree Analysis, Dependence Diagrams, Markov Analysis, and Common Cause Analysis.

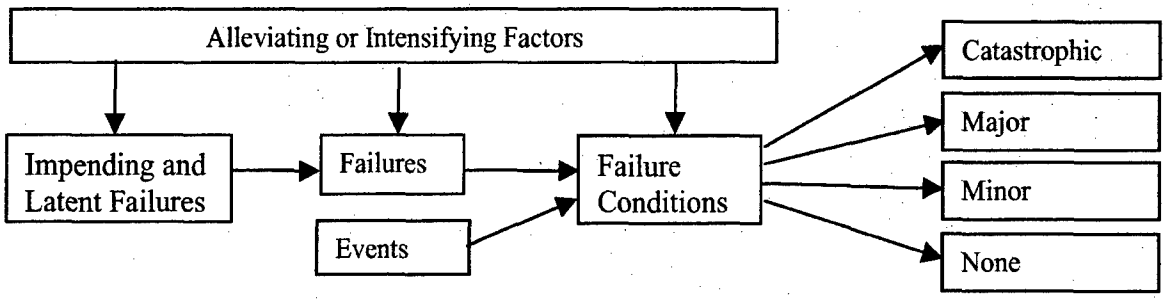

Figure 1: elements of the Failure Hazard Analysis

Figure 2 shows a flowgraph identifying the generic decision logic guiding the use of analysis techniques.

In-Service Risk Assessment

Though certification requirements mandate a thorough safety analysis prior to an aircraft's introduction to service, changing service profiles, subsystem modification, and unanticipated failure modes may effect the applicability of the original analysis. During evaluation of service problems, the focus of the investigation may narrow to parts, components, and subsystems. Under these conditions studying the original safety analyses may identify basic design weaknesses and help interpret the service event. A full re-analysis of the system is often not necessary and is impractical.

Where service history indicates a potential threat associated with degraded components in the EIS, remedial action needs to be taken and, if necessary, will be mandated by an Airworthiness Directive (AD). The remedial action may come in the form of operational restrictions, maintenance or inspection requirements, or aircraft modification. In any case, the remedy must be preceded by an analysis that conservatively estimates the probable frequency, severity, and exposure of the threat.[2] Wholesale re-assessment of the EIS to current standards of FAR 25.1309 may be a possibility, but is almost certainly not very practical and to a large degree redundant with prior analysis. Data collection would be extremely difficult (even for aircraft with few modifications) and the results of the analysis might not indicate practical means for upgrading the particular components of EIS.
These circumstances demand that the risk tools used by aircraft operators be sufficiently flexible to admit alternative data sometimes at a much more general level. One approach to risk abatement of an older EIS is to perform a risk analysis, utilizing service data, in addition to fault trees and other standard techniques, to narrow the focus on evidential safety threats. In January of this year, the Aging Transport Systems Rulemaking Advisory Committee's Intrusive Inspection Working Group (IIWG) published a report with such an analysis.

Note: The FAA is examining several concepts for facilitating compliance with existing and emerging rules regarding electrical systems safety assessment. The following approach represents neither a proposed change to the rules nor an approved means of compliance with those rules.

The IIWG Methodology

The IIWG was tasked with determining the state of wire on six decommissioned aircraft and assessing the risks associated with the wire flaws if those aircraft had been operating with those flaws. Because the IIWG's intention was to identify generic threats to the EIS (not specific conditions correctable by service bulletin or AD) and because the IIWG did not have complete design or configuration data on the EIS inspected, there was

[2] In a policy statement published in the Federal Register, July 2, 2001, the FAA stated that simple reliance on standard or best practice (including AC 43-13) was not sufficient for regulatory approval of a type design data package.

no effort to identify the specific threat associated with the conditions found. Instead, the IIWG identified generic conditions and postulated the risk associated with certain hypothetical (but realistic) situations surrounding those conditions.

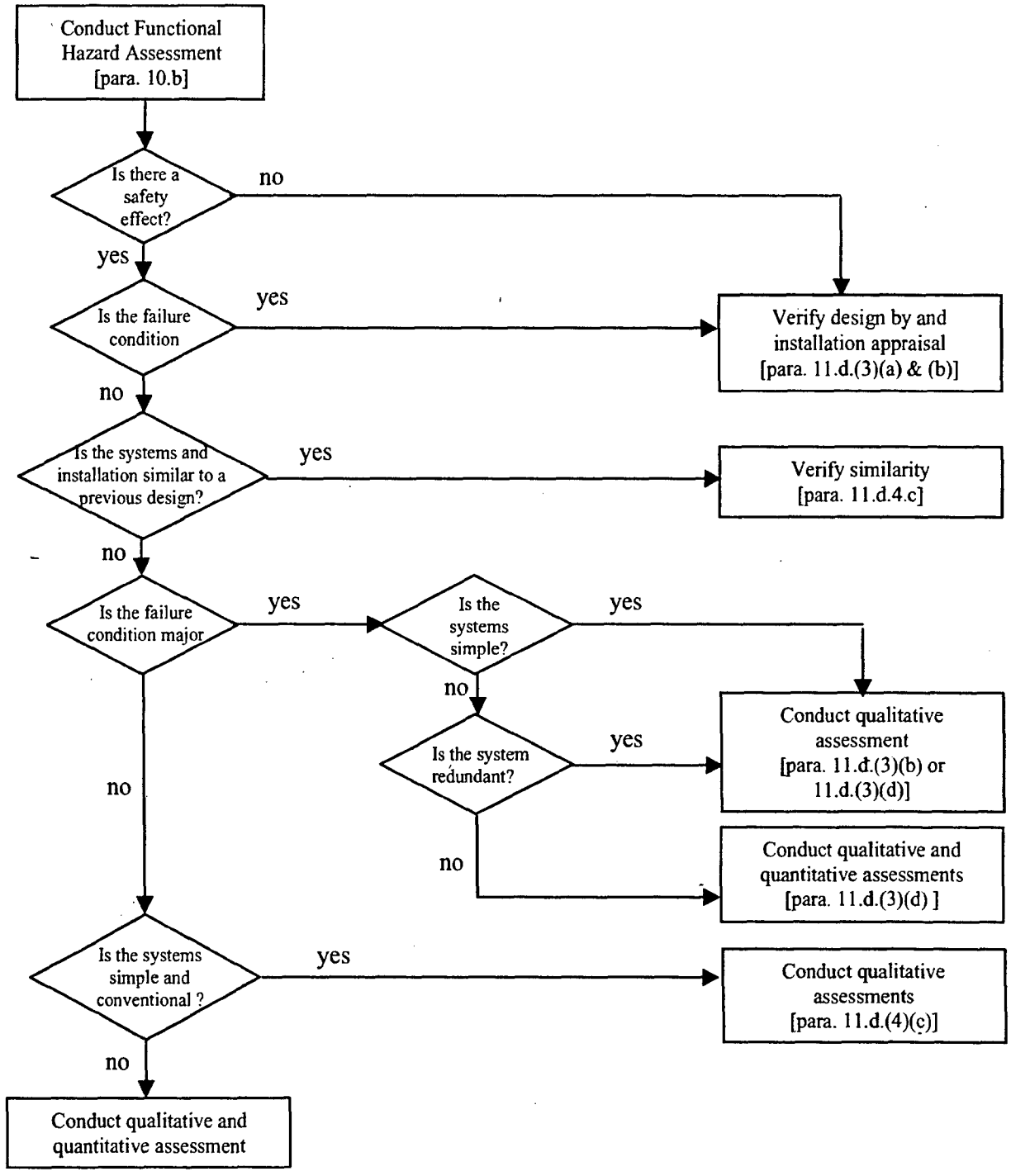

Figure 2: Depth of Analysis Flowchart

Despite its rather unique risk assessment objectives, the IIWG did base its methodology upon industry-accepted subsystems risk analysis. In order to conduct a System Safety Assessment, the analyst requires knowledge of at least the following four parameters:

- Failure Identification
- Failure Effect
- Probability of Occurrence
- Failure Condition Severity

In the aircraft design phase, the full availability of design specifications allows the failure condition severity and effects to be determined in an often lengthy but conceptually simple analysis (the FHA and derived safety requirements from the preliminary system safety assessment). On the other hand, the absence of relevant service data requires the use of sophisticated analysis techniques, testing and expert judgment to estimate the probability of occurrence (a systems safety assessment using FMEA, Fault Trees, etc).

Just the opposite was true for the IIWG assessment of the decommissioned aircraft. For the IIWG the probability of occurrence was relatively easy to assess from the frequency of the findings. On the other hand, because the conclusions the IIWG would generate were to pertain to generic subsystems and because the findings were often latent flaws or flaw precursors, the failure condition and effects were much harder to assess. As such, the IIWG developed a modified FHA and systems safety assessment referred to as the General Threat Analysis (GTA).

In the GTA, conditions (flaws and flaw precursors) were assessed for severity given plausible, hypothetical situations[3]. Hypothetical situations involve subsystems characterized, not by function and design, but by a set of factors, which would aggravate the degeneration of conditions into hazardous failures. The GTA begins with the development of two lists:

- A listing of the significant wire condition. In the case of the intrusive inspections, these observations were the direct result of the inspections. For revenue service aircraft, this data can be generated by inspection or by service difficult review.
- A listing of all generic conditions, which may aggravate – in any plausible situation – a failure associated with the terminal condition of any observed degenerative condition. Note that this list does not necessarily include factors that may have led to or may yet advance the condition; only those factors that could make some presumed subsequent failure more or less severe.

The two lists produced by the IIWG are presented in Tables 1 and 2. Table 1 contains only age-related wire conditions. For more comprehensive analyses, a larger and more detailed list would be created. Similarly, Table 2 contains only approximate aggravating conditions. A more precise analysis would require a more detailed list.

The two lists and the expertise and experience of the IIWG members were used to develop generic fault graphs. These fault graphs indicated the severity of the potential (worst case) consequence, if the fault were allowed to reach its fully degenerate state. Each branch of the fault graph terminated in one of three possible severities[4].

> Undesirable – any condition that might – if left uncorrected – lead to a slight reduction in safety margins, slight increase in crew workload, or inconvenience to the occupants.
>
> Severe – any condition that might – if left uncorrected – lead to significantly reduced safety margins or functional capabilities, a significant increase in crew workload impairing crew efficiency, or substantial discomfort to occupants.

---

[3] Plausible hypothetical situations will be those situations supported by the existence of data for that or a similar situation and/or the expert opinion that such situations could reasonably be expected to occur in the life of an aircraft.

[4] The fault graphs did not need to terminate in only three possible severities, but any such analysis must not have more terminal conditions than the resolution of the analysis permits. In other words, if there were 100 possible terminations, the analysis must be sufficiently sensitive to clearly and consistently distinguish between the 87th and 88th terminal condition.

Critical – any condition that might – if left uncorrected – lead to a large reduction in safety margins or functional capabilities, higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely, or adverse affects upon occupants.

Wire Condition	Definition
Deteriorated Repair	A faulty wire splice assumed to have met requirements when established (e.g., a splice originally established to be environmentally sealed but no longer so).
Heat Damage or burnt wire	Thermal damage to insulation resulting from the presence of elevated temperature due to internal or external heating.
Vibration Damage/Chafing	Insulation wear (material loss) resulting from the repeated application of a force which, if applied only once, would not result in noticeable damage.
Cracked Insulation	A breach in the wire insulation that does not include breaches resulting from the direct physical contact or traumatic force (e.g., knife cut or tears).
Arcing	One or more instantaneous electrical discharges evidenced by burnt spot on one or more wires and melted conductors.
Delamination	The unraveling of a tape-wrapped insulation. The separation of layers of insulation in a multilayered construction.

Table 1: age-related wire conditions

Aggravating Condition	Definition
Explosive Environment	An environment where there is a reasonable expectation of the presence of an explosive combination of gases during some phase of operation.
Flammable Materials	Surrounding materials that can sustain combustion. Includes the wire insulation itself (e.g., PVC but not polyimide).
Other Critical Systems	The wire in question is bundled with other wires, at least one of which supplies current or signals to systems required for safe flight.
Moisture	Normal relative humidity in excess of 90% during some phase of flight (landing, takeoff, climb, cruise, decent, approach, landing), resulting in enhanced likelihood of shorting.
Vibration	Sufficient relative motion between wires or between wires and structure to cause or accentuate intermittent shorting.
Contamination	Contamination as the result of normal operation or maintenance resulting in either enhanced flammability or likelihood of shorting.
Cockpit or Electronics Compartment	High consequence failure locations within the aircraft.
Arc Tracking Potential	The presence arc-track-susceptible materials in the bundle in conjunction with those conditions which could precipitate sustained arcing.
Potential for Excessive Resistance Heating	Wires with high current loads may fail as the result of excessive resistive heating at repair or splice locations. This failure can evolve into severely burnt, cracked, or melted insulation on the offending wire and its neighbors. With excessive heat and bare wire at these locations, the potential for fire is high.

Table 2: aggravating conditions

The fault graph was assembled by using the IIWG's expert judgement to identify the most significant aggravating condition[5]. The presence or absence of this condition leads to the first branch. The presence of successively important aggravating conditions was assessed until either the combined conditions necessarily resulted in an extreme outcome (critical or undesirable) or until all aggravating conditions were exhausted.[6] The fault graphs were further simplified by eliminating branches that necessarily lead to the same outcome. The fault graphs and flaw frequency data were then used to develop the IIWG's recommendations for EIS risk elimination or mitigation.

Having established the presence of an unacceptable condition, the aircraft designer may work backward or forward through the fault graph to identify interventions. For example, if the path through the fault graph in Figure 3 terminates immediately after the block that assesses the presence of vibration, the designer may force the terminal condition from "severe" to "undesirable" (less severe) by modifying the wire harness support hardware and ensuring protection from contamination

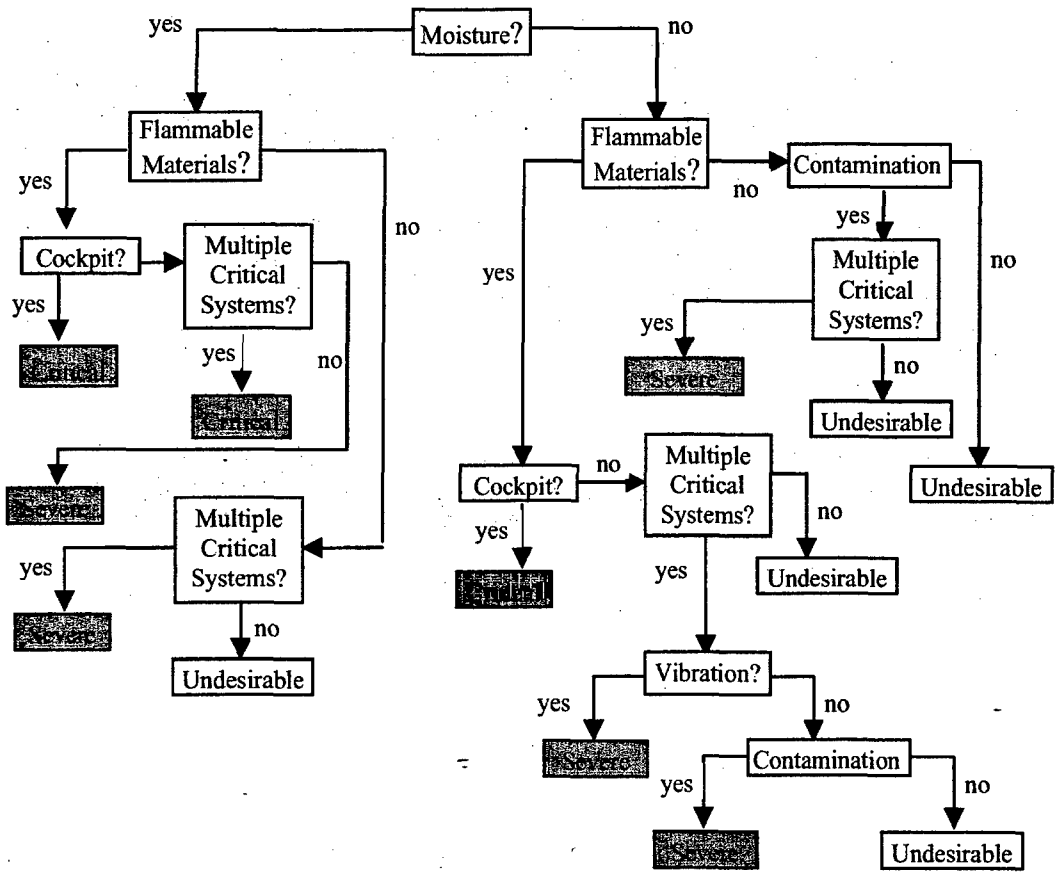

Figure 3: Example Fault graph for Wire Cracking

[5] The most significant aggravating condition depended somewhat on the wire fault under consideration. In general, it turned out to be the presence of moisture, but not always.

[6] Consideration of the aggravating conditions in order of importance is only necessary to minimize the complexity of the resulting fault graph. An arbitrary order should (if the same decision criteria are applied) lead to the same outcomes, though with more branches (i.e., redundancy).

Enhanced Risk Assessment Tools

Drawing from both standard design practice and the IIWG's risk assessment methodology, the FAA has initiated a project to develop risk assessment tools for application to existing EIS. The end product is expected to be an analysis methodology implemented in computer software that is:

> ***Relevant:*** Model assumptions cannot be brushed off as simple parameters that can be changed as necessary. A risk model has no virtue if its assumptions are unjustifiable or parameters unknown or unavailable.
>
> ***Practical:*** The end users of the risk assessment tools developed under this program will most likely be airline engineering and maintenance organizations. The risk assessment tools will have no virtue if the end users cannot embrace the tools because they are too complicated or because the tools seriously violate constraints of their operations (e.g., require unavailable data).
>
> ***Useful:*** The tools should do more than confirm the obvious.

The IIWG fault-tree methodology was developed for the specific purpose of analyzing the intrusive inspection data. Because it was created in the course of the intrusive inspection project for the sole purpose of analyzing data from those inspections, it could be (and had to be) simple and reliable. In developing a more general methodology for application to revenue service aircraft, the FAA has the same requirements for high reliability but a greater need for broader applicibility.

Furthermore, the availability of design data for revenue service aircraft should be better, and the availability of configuration and modification data should be complete. Hence, while the risk analysis may not be able to quantify the risk of one specific wire in a bundle arcing to another specific wire, it should be able to quantify the risk of a newly installed in-flight entertainment wire acring to a wire in an adjacent bundle that is known to support flight critical subsystems.

Concluding Remarks

The FAA is committed to reducing the risks associated with electrical interconnect system failures. In doing so, the FAA is pursuing a program to develop risk assessment tools suitable for application to aging revenue service aircraft. The tools will support routine modification and configuration control as well as remedial action in response to safety threats.